Joint Hearing Before the Committee on Governmental Affairs and the Subcommittee on Oversight of Government Management, Restructuring and the District of Columbia United States Senate

---

For Release on Delivery
Expected at
10:30 a.m. EST
Wednesday
November 14, 2001
Report Number: CC-2002-038

Status of Airline Security After September 11, 2001

Statement of
The Honorable Kenneth M. Mead
Inspector General
U.S. Department of Transportation

Chairmen Lieberman and Durbin, Ranking Members Thompson and Voinovich, and other Members of the Committee:

We appreciate the opportunity to testify on improvements to aviation security since September 11, 2001, and improvements that still need to be made. The Federal Aviation Administration (FAA) and Department of Transportation (DOT) have taken steps to tighten security, and our observations across the country confirm that security is noticeably tighter than before September 11th.

FAA issued additional security requirements that air carriers and airport operators must implement to improve aviation security. These requirements included, but were not limited to, comparing the names of passengers and individuals with airport identification with the Federal Bureau of Investigation's watch list, intensified passenger and carry-on baggage screening at security checkpoints, limiting access beyond the screening checkpoints to passengers with tickets or ticket confirmations, "continuous use" of explosives detection systems used to screen passengers' checked baggage, revalidating airport identification required to access secure areas of the airport, and increasing law enforcement presence at screening checkpoints.

The Department has also taken several measures to provide protection to commercial aircraft and the Nation's airports. One such measure included expanding the Federal Air Marshal program for both domestic and international flights. Another measure provided for deployment of National Guard troops by State Governors to reinforce security at passenger screening checkpoints at airports nationwide.

Despite existing and new security requirements there are still alarming lapses of security and some systemic vulnerabilities that need to be closed. The President, the Secretary, and Attorney General have called upon the DOT Office of Inspector General (OIG) to assist in oversight of airport and aircraft security. On November 9, 2001, the President instructed the DOT Office of Inspector General to "conduct undercover audits" of security performance at airports nationwide, to ensure strict compliance with FAA security requirements. We have conducted such audits in the past, and our teams will be in place before Thanksgiving weekend. As part of this effort, we will conduct a variety of observations and tests to measure compliance with current FAA security requirements.

The Secretary announced on October 30, 2001, that joint teams of FAA and OIG personnel would monitor screening operations at airports nationwide in support of his zero tolerance policy. Since this announcement, over 100 OIG personnel have conducted security observations at 58 airports nationwide.

During these observations, our office and FAA found instances where air carriers were not continuously using explosives detection systems to screen checked baggage, staff at screening checkpoints were not identifying dangerous items such as knives in passenger carry-on baggage, and air carriers were not randomly screening passengers boarding aircraft. Since November 3, heightened security efforts have resulted in numerous—often unprecedented—actions taken when security has lapsed or been breached. Actions taken by FAA include deplaning and concourse evacuations, followed by rescreening of all passengers. To date, approximately 90 such incidents have occurred.

We think the Secretary's zero tolerance policy is for the best, and much needed under the circumstances. If security lapses are found during OIG and FAA observations, the Secretary has authorized concourses to be evacuated and passengers rescreened. Although this will occasionally result in delays or inconvenience to passengers, it is in the best interest of the aviation security system and shows that there will be consequences for industry's noncompliance with FAA security requirements. It will demonstrate to air carriers and screening companies that it is more efficient and effective to do it right the first time.

Given the scope, complexity, and dynamics of the security challenge as we now know it, coupled with long-standing problems with the aviation security program, we believe fundamental changes are needed to enhance the effectiveness of the aviation security system. First and foremost, aviation security must reside in a single entity with security as its primary and central focus, profession, and mission. A centralized, consolidated approach by an organization with a security mission would require passenger and baggage screeners to have uniform, more rigorous training and performance standards nationwide. This organization must also work toward 100 percent screening of checked baggage and cargo. It should be noted that bulk explosives detection equipment must be integrated into the airport/air carrier baggage systems. FAA needs to make this a top priority in order to screen 100 percent of checked baggage.

Both the House and Senate have legislation that address fundamental changes that are necessary in order to improve the Nation's aviation security system. It is particularly noteworthy that the Senate Bill includes provisions for the Department to set measurable goals and objectives for aviation security consistent with the Government Performance and Results Act of 1993. Any change in the governance and organization of our aviation security system cannot be done overnight and will require a transition period. In the interim, we must enhance the current system and improve security measures now in place.

While aviation security has been tightened since September 11th, there are still some vulnerabilities that need to be addressed without delay. Our office and the

General Accounting Office (GAO) have issued numerous reports identifying weaknesses in the aviation security system and recommending corrective actions. Chief among the actions that FAA needs to take are:

- Ensure air carriers maximize the use of bulk explosives detection machines for screening of passengers' checked baggage. Air carriers are now required to continuously use bulk explosives detection machines. That means that the carriers are required to randomly select enough passengers with checked baggage to supply the machine with a constant stream of bags to examine. However, during our recent observations, the majority of air carriers were not selecting enough passengers to supply the machines with a constant stream of bags. In contrast, at one airport an air carrier was requiring all checked baggage to be screened. We also observed instances were the check baggage screening operations were not adequately staffed. As a result, one air carrier had to stop operating the machine. Before FAA issues its final rule on checked baggage security on flights within the United States, it needs set a minimum usage level (number of bags screened per day) for the machines and address staffing issues.

- Issue the final rule on certification of screening companies to improve the screening of passengers, baggage, and cargo. The Federal Aviation Reauthorization Act of 1996 directed FAA to certify screening companies and improve screener performance. FAA was prepared to issue its final rule the week of September 10, 2001. Following the September 11th tragedy, the Department elected to delay the final rule so the Rapid Response Teams could re-evaluate the certification requirements. Once issued, this rule will serve as the baseline for ensuring the quality of screening, whether it is performed by Federal or contract employees.

- Establish standards for measuring security screener performance based on computer-assisted testing and unannounced testing of screeners by FAA. It is important that performance standards be established for screeners, whether they are Federal or contract employees. If such standards are not met employees shall be terminated.

- Strengthen controls to prevent access to secure areas of the airport by unauthorized individuals. Our testing in this area has shown serious weaknesses in the past. During late 1998 and early 1999, we successfully accessed secure areas[1] in 68 percent of our tests at eight major U.S. airports.

[1] OIG uses the term **secure area** to define the area of an airport where each person is required to display airport-approved identification, such as the area where an aircraft is parked. Each airport defines this area, which may be the entire Air Operations Area or may be limited to a smaller, more restrictive area.

Once we entered secure areas, we boarded aircraft 117 times. The majority of our aircraft boardings would not have occurred if employees had taken the prescribed steps, such as making sure doors closed behind them. Since September 11th, FAA has required the airports to reduce the number of access points to secure areas of the airport. This is one area we will be testing as directed by the President.

- Conduct criminal history checks for all individuals, including current employees, who have unrestricted access to secure areas of the airport. This is currently being done for all new employees at Category X airports. FAA has also required airports to revalidate all airport identification, but this does not require background investigations or criminal history checks to be conducted for individuals currently holding airport identification. Our recent investigations have found that individuals who have been convicted of disqualifying felonies possessed airport identification, allowing them access to secure areas of the airport. The requirements must be expanded to all airports not just the large ones. Criminal history checks must also be performed on all individuals that currently have airport identification, as well as new employees.

- Strengthen controls in cargo security, particularly the process for certifying indirect air carriers[2] (freight forwarders) and assessing indirect air carriers' compliance with cargo security requirements. We recently completed a follow-up audit of FAA's Cargo Security Program and briefed FAA on our results in September. FAA has taken action to strengthen the program since September 11th, by no longer allowing air carriers to accept cargo from unknown shippers and strengthening the requirements for becoming a known shipper.

[2] An indirect air carrier is any person or entity, excluding an air carrier, that engages indirectly in the transportation of property by air, and uses the services of a passenger air carrier. This does not include the U.S. Postal Service.

Today, I would like to highlight those steps taken by the DOT and FAA to enhance both airport and aircraft security, and share with the Committee our observations on the execution of such steps by air carriers and airport operators who are ultimately responsible and accountable for the security of air travelers. I would also like to address specific fundamental changes that are needed to further strengthen aviation security and hopefully restore public confidence in air travel.

Actions Taken to Tighten Aviation Security

Immediately following the terrorist attack of September 11th, DOT and FAA, initiated a variety of security requirements necessary for protecting aircraft and passengers, as well as airports and their users from future terrorist attacks.

FAA first ordered all airport terminals evacuated and required a thorough physical search for explosives and other dangerous weapons, using airport personnel and FAA-certified canine teams. FAA then imposed an initial set of security directives that airport operators and air carriers had to certify were in place before the airports could reopen and flights could resume. This process was completed on September 14th, and scheduled commercial service was resumed to all the Nation's airports except Reagan National Airport.

The Secretary announced, on September 16th, the creation of two Rapid Response Teams to review and provide recommendations for improving aviation security. One team focused on increasing airport security, while the other team focused on securing the aircraft, particularly access to the cockpit. The teams included senior DOT and FAA officials, and industry representatives.

Several of the recommendations from the Rapid Response Team's report have already been implemented by FAA, such as limiting carry-on items to one carry-

on bag and one personal item (purse or briefcase), and requiring airports to revalidate airport identification. Also, many of the recommendations of the Rapid Response Teams were included as part of congressional legislation that is currently being considered by members of the Senate-House conference committee on transportation/aviation security.

Also, air carriers are securing cockpit doors in response to the Rapid Response Team recommendation. FAA is working with the air carriers to ensure all cockpit doors are secured and that modifications do not affect the safety of the aircraft. The Air Transport Association (ATA) recently reported that 100 percent of the cockpit doors on its members' fleets have been secured. That equates to 97 percent of the passenger aircraft in the system. Many non-ATA member airlines have also reported they have secured the cockpit doors on their fleets.

Some of the initial security requirements imposed by FAA have been lifted or revised, such as the ban on curbside check-in and the ban of all cargo and mail on passenger aircraft. At the same time, several initial requirements remain in effect or have been strengthened and new requirements have been added. These include requirements such as:

- A comparison of the names of passengers and individuals with airport identification with the Federal Bureau of Investigation's watch list.
- Continual use of bulk explosives detection systems for screening passengers' checked baggage.
- A ban on cargo from unknown shippers.
- Strengthened requirements for becoming a known shipper of cargo.
- Allowing only ticketed passengers and authorized persons to proceed past screening checkpoints.

- Searching aircraft at the beginning of each day.
- Conducting random physical searches of passengers prior to boarding the aircraft.

While FAA has tightened aviation security with the new and revised requirements, the challenge is to ensure that air carriers, screening companies and airports comply with the new requirements.

Coinciding with the issuance of FAA's security requirements, FAA has also expanded the Federal Air Marshal program for both domestic and international flights. Law enforcement personnel from several Federal agencies, including the OIG, have been selected and trained to augment the Federal Air Marshal program until such time as FAA can recruit and train the necessary personnel. We think it is a wise decision to substantially increase use of this program in the interest of restoring public confidence and as a deterrent to future attacks on aviation.

National Guard troops have been called by State Governors to reinforce security at passenger screening checkpoints at airports nationwide. Since September 11th, more than 6,000 members of the National Guard have been mobilized at airports nationwide. On November 9, 2001, the President called for an increase of 25 percent in Guard personnel during the holidays. In addition to its initial order to monitor passenger and baggage screening, Guard members will also monitor activity at boarding gates, search vehicles and cars, and monitor curbside activity.

The President, the Secretary, and the Attorney General have called upon the DOT Office of Inspector General to assist in oversight of airport and aircraft security. On October 30, the Secretary announced that joint teams of FAA and OIG personnel would begin monitoring screening operations at airports nationwide in support of his zero tolerance policy.

We think the Secretary's zero tolerance policy is for the best, and much needed under the circumstances. If security lapses are found during OIG and FAA observations, the Secretary has authorized concourses and planes to be evacuated and passengers re-screened. Although this will occasionally result in delays or inconvenience to passengers, it is in the best interest of the aviation security system and shows that there will be consequences for industry's noncompliance with FAA security requirements. . It will demonstrate to air carriers and screening companies that it is more efficient and effective to do it right the first time.

On November 9, 2001, the President instructed the DOT Office of Inspector General to "conduct undercover audits" of security performance at airports nationwide, to ensure strict compliance with FAA security standards. We have conducted these audits in the past and our teams will be in place before Thanksgiving weekend. As part of this effort, we will conduct a variety of tests and observations to measure compliance with current FAA security requirements.

Despite the Recent Security Enhancements, Lapses in Aviation Security Continue to Occur

Since September 11th, the dynamics of aviation security continue to change based primarily on the latest information from the intelligence community. This has prompted FAA to review and update, if necessary, its latest security requirements. FAA has also modified its security requirements based on its own oversight of air carrier and airport operator.

However, since FAA's new security requirements went into effect following September 11th, there are two areas of security where execution of such

requirements has not been as effective as it should be: screening checkpoint and checked baggage security. Historically, these two areas of security have been the weak link in aviation security. Even with improvements in technologies used to screen passengers, carry-on bags and checked baggage, lapses still occur at screening checkpoints and in checked baggage security as evidenced by our recent observations at airports nationwide.

Screening Checkpoint Security

Since the terrorist attacks of September 11th, OIG has carried out several initiatives to assess airport security. First, on September 14th, 3 days following the terrorist attacks, we arrested 12 non-U.S. citizens who illegally obtained security badges to gain admittance to secure areas at a major U.S. airport.

On October 12th, at the request of the Secretary, a joint team of OIG special agents and FAA security specialists was dispatched to Philadelphia International Airport to scrutinize screening operations conducted by Argenbright Security and to ensure that Federal security requirements were being enforced. In May 2000, an OIG investigation culminated in three Argenbright managers pleading guilty to falsifying documents about screener background checks. The firm was placed on 3 years probation and ordered to pay over $1 million in fines and restitution for failing to conduct background checks and falsifying screener training records. The case was prosecuted criminally at the urging of the OIG, based on the overwhelming evidence that Argenbright and its managers had systematically defrauded FAA's regulatory security program.

Because the October 12th investigation found that shoddy practices in the hiring and training of security screeners continued to exist, the Secretary and Attorney General directed the OIG to conduct similar investigations at 13 other airports

where Argenbright performed security services. A random sample of Argenbright employees at these airports found cases where employees (1) were not able to pass a skills test, administered on-the-spot by OIG personnel, required for employment, (2) had criminal records disqualifying them from employment as screeners, or (3) were foreign nationals not authorized to work in the United States.

On October 22nd the U.S. Attorney's Office and Argenbright entered into an agreement whereby Argenbright admitted violating terms of its probation and agreed to a series of remedial actions, to include extending its probation to 5 years and conducting fingerprint checks on all of its employees not previously checked by the OIG.

On November 9, 2001, Argenbright Security announced major overhauls in the Company's management and "…immediate measures to ensure that Argenbright meets and exceeds the public's and Administration's heightened security expectations." The Company stated these measures will introduce training that meets European standards and will lead to the immediate termination of employees who do not follow strict procedures and regulatory guidelines. The Company announced that all 7,000 Argenbright employees will undergo background re-verification and fingerprint checks in cooperation with the FAA, FBI, and air carriers.

As directed by the Secretary, joint teams of FAA and OIG personnel began monitoring screening operations at airports nationwide. If security lapses were found during the agents' observations, the Secretary authorized terminals to be evacuated and passengers re-screened, as part of his zero tolerance policy. FAA has reported several security breaches at passenger screening checkpoints at airports nationwide. Most recently, at Chicago's O'Hare International Airport, a

passenger was able to enter the boarding area through a United Airlines passenger screening checkpoint carrying pepper spray, seven knives and a stun gun.

Between November 3 and November 12, 2001, over 100 OIG personnel conducted observations at 58 airports nationwide. During these observations, we found that the private firms performing screening checkpoint security on behalf of the air carriers were not consistently and uniformly following FAA's security requirements. Often the problems occurred because screeners were not aware of or did not understand the new FAA requirements. Examples of where FAA requirements were not being followed include:

- Checking Identification at Screening Checkpoints. In some cases, passengers' identification were not checked against their boarding passes or employees' airport identification was not verified at the screening checkpoint. Passengers or employees were allowed beyond the screening checkpoint without their identification being checked.

- Screening Carry-on Items. Some screeners were not adequately screening carry-on bags for threat items (knives, scissors, sharp objects, etc.), or separately screening laptop computers from the passengers' carry-on bags. As a result, prohibited threat items that were missed during the initial screening were found in passengers' carry-on bags during secondary screening at the departure gates.

- Random Screening of Passengers and Carry-on Items. We also observed some screeners not performing continuous random secondary screening procedures of passengers and their carry-on items. These secondary screening procedures include physical searches of carry-on items, using trace explosives detection devices to screen carry-on items, and screening passengers using body wands

or pat down techniques. At some security checkpoints we observed, these secondary screening procedures were not being continuously performed.

Since November 3, heightened security efforts have resulted in numerous—often unprecedented—actions taken when security has lapsed or been breached. Actions taken by FAA include deplaning and concourse evacuations, followed by rescreening of all passengers. To date, approximately 90 such incidents have occurred.

For example, in one instance a passenger at Baltimore-Washington International Airport was charged with testing security screening on her own with a box-cutter concealed within a make-up kit in her purse. After clearing the initial screening checkpoint, the passenger allegedly produced the instrument, announcing that the screeners failed her test and that security at the airport was unacceptable. Since the passenger was not detained by the screeners, the concourse was evacuated and all passengers were rescreened. While airport police eventually found the passenger, it resulted in a 3-hour delay adversely affecting at least 27 flights. OIG special agents presented the case to the U.S. Attorney's Office, which charged the individual with a misdemeanor for knowingly and willfully entering an airport area in violation of security requirements.

In another case, OIG special agents detected an individual at Dulles International Airport sneaking a pocketknife in his shoe through a checkpoint after having been previously warned by a screener to discard the knife. OIG special agents arrested the individual on a felony charge.

Judicial disposition in both cases remains pending. The Secretary has stated that these practices will not be tolerated and the airlines should be prepared to have penalties assessed if these practices continue.

Checked Baggage Security

We have deployed OIG personnel at airports nationwide to observe the screening of checked baggage. Following September 11th , FAA requires air carriers to ensure that bulk explosives detection machines are in continuous use. Specifically, FAA requires air carriers to randomly select enough passengers with checked baggage to supply the machine with a constant stream of bags to examine. Results from our preliminary observations at seven major airports in October 2001 found that most air carriers were not continuously using the machines to screen checked baggage. This prompted us to continue monitoring the use of these machines.

Today, we continue to find that the air carriers are not maximizing the use of these machines. We continue to find instances where the machines are woefully underutilized and understaffed, and when they are being used, FAA's security requirements were not being followed. Over the past holiday weekend, we conducted 115 observations of 30 machine (1 machine could have more than 1 observation) at 9 airports during high, steady and low passenger traffic at check in counters. Our observations found that 73 percent of the machines were not in continuous use.

For example, during a 30 minute observation, 62 passengers checked baggage, but only 7 bags were screened through the machine. In contrast, we observed one carrier that required all checked baggage be screened.

Underutilization of these systems has been a long-standing problem that we have reported on since 1998. These machines cost approximately $1 million to buy, and have cost between $300,000 and $1.2 million to install. Before the events of

September 11th, there were various reasons why these machines were underutilized. One of the overriding reasons was that air carriers were only required to use the equipment to screen the baggage of passengers requiring additional security measures based on a passenger prescreening system known as the Computer Assisted Passenger Prescreening Systems (CAPPS). Air carriers' reluctance to increase the use is centered in their belief that passengers would not accept the inconvenience.

In our October testimony before the House of Representatives, Committee on Transportation and Infrastructure, Subcommittee on Aviation, we stated that during the month of July the majority of machines continue to be underutilized.

Screening Rates of 80 CTX 5500 Machines Installed in U.S Airports During July 2001	
Number of CTX Machines	**Bags Screened Per Day**
07	0-100
16	101-200
31	201-400
14	401-600
06	601-800
06	801-1200

These machines are capable of screening between 140 and 150 bags per hour in an operational environment. FAA needs to take immediate steps to ensure that air carriers use the equipment at this level.

We also found incidents where the checked baggage screening operations were not adequately staffed. FAA requires all bags that set off the screening machine's alarm must be physically searched and screened using trace explosives detection devices. At many airports, these machines are staffed with one operator to perform the screening operations when in fact at least two screeners should be

required. The operator responsible for screening the bag through the machine should not be solely responsible for threat resolution, i.e. trace and physical search. It is not just a matter of passenger inconvenience but of security effectiveness. One operator performing all screening responsibilities without any assistance will generally cut corners (i.e., bypass the trace and physical search requirements) not to inconvenience a line of passengers.

We also found that there were not always enough trained operators to effectively staff checked baggage screening operations. For example, at one airport, the private security firm responsible for screening checked baggage, on behalf of one air carrier, had only two trained screeners to operate the machine. These screeners were working 10-hour shifts, 6 days a week, and a 20-hour shift on the other screener's day off. During our observation of machine operations on the morning of November 12, we witnessed the screener falling asleep. The screener was scheduled for a 20-hour shift while just completing a 10-hour shift from the prior day. We alerted the private security firm and responsible air carrier officials, who stopped operating the machine, since another qualified operator was not available.

Fundamental Changes Are Paramount to the Success of an Effective Aviation Security System

Given the scope, complexity, and dynamics of the security challenge as we now know it, coupled with long-standing problems with the aviation security program, we believe fundamental changes are needed to enhance the effectiveness of the aviation security system. These fundamental changes include creating a single entity responsible for the aviation security system, and correcting existing weaknesses in the system such as inadequate training and performance standards for screeners.

First and foremost, there should be an end to the practice of shared aviation security responsibilities among the Government, air carriers, and airports. This practice has not worked in the past and will not worked in the future. There are simply too many other priorities, missions, and, in some cases, competing economic pressures for air carriers and airports.

Aviation security, must reside in a single entity with security as its primary and central focus, profession, and mission. A centralized, consolidated approach by an organization with a security mission would require passenger and baggage screeners, whether Federal or contract employees, to have uniform, more rigorous training and performance standards nationwide. The employees of this entity would be required to meet established performance standards and would be subject to termination if they do not perform. This should result in more consistent security at our Nation's airports.

This entity would also be able to maintain close ties to the intelligence community; revise requirements or procedures without going through a lengthy rulemaking process; require employees to be U.S. citizens and have background and credit checks; and provide screening personnel better salaries and a career path.

Any change in the governance and organization of our aviation security system cannot be done overnight and will require a transition period. In the interim, we must enhance the current system and ensure compliance with security requirements now in place.

Second, while aviation security has been tightened since September 11th , there are still some vulnerabilities that need to be addressed without delay. Our office and

the GAO have issued numerous reports identifying weaknesses in the aviation security system and recommending corrective actions. FAA needs to take the following immediate actions:

- Ensure air carriers increase use of bulk explosives detection machines for screening of passengers' checked baggage, and issue the final rule on security procedures for checked baggage on flights within the United States. Air carriers are now required to continuously use bulk explosives detection machines, but during our recent observations the majority were not running bags continuously through the machines. Before FAA issues its final rule on checked baggage security on flights within the United States, it needs set a minimum usage level (number of bags screened per day) for the machines and address staffing issues.

- Issue the final rule on certification of screening companies to improve the screening of passengers, baggage, and cargo. The Federal Aviation Reauthorization Act of 1996 directed FAA to certify screening companies and improve screener performance. FAA was prepared to issue its final rule the week of September 10, 2001. Following the September 11th tragedy, the Department elected to delay the final rule so the Rapid Response Teams could re-evaluate the certification requirements. Once issued, this rule will serve as the baseline for ensuring the quality of screening, whether performed by Federal or contract employees.

- Establish standards for measuring security screener performance based on computer-assisted testing and unannounced testing of screeners by FAA. It is important that performance standards be established for screeners, whether they are Federal or contract employees. Standards must be established for

screeners, and continued employment must be based on each individual meeting those standards.

- Strengthen controls to prevent access to secure areas of the airport by unauthorized individuals. Our testing in this area has shown serious weaknesses in the past. During late 1998 and early 1999, we successfully accessed secure areas in 68 percent of our tests at eight major U.S. airports. Once we entered secure areas, we boarded aircraft 117 times. The majority of our aircraft boardings would not have occurred if employees had taken the prescribed steps, such as making sure doors closed behind them. Since September 11th, FAA has required the airports to reduce the number of access points to secure areas of the airport. This is one area we will be testing as requested by the President.

  FAA recently issued regulations making individuals directly accountable to FAA for noncompliance with access control requirements, but testing and assessing fines for security violations is not the only answer. FAA must assist airport operators and air carriers in developing and implementing comprehensive training programs. All security training programs, not just for access control, must teach employees their role in aviation security, the importance of their participation, how their performance will be evaluated, and what action will be taken if they fail to perform.

- Conduct criminal history checks for all individuals, including current employees, who have unrestricted access to secure areas of the airport. This is currently being done for all new employees at Category X airports. FAA has also required airports to revalidate all airport identification. However, this does not require background investigation or criminal history checks to be conducted. Our recent investigations have found that individuals who have

been convicted of disqualifying felonies had airport identification, allowing them access to secure areas of the airport. We must expand the requirements and conduct criminal history checks on all individuals currently holding airport identification, as well as new employees at all airports nationwide. We must also look for alternative methods of confirming the trustworthiness of individuals with access to secure areas of the airport, especially individuals who have not been in the United States long enough for a criminal records check to be effective.

- Strengthen controls in cargo security, particularly the process for certifying indirect air carriers (freight forwarders) and assessing indirect air carriers' compliance with cargo security requirements. In 1997, we advised FAA of the need to strengthen the indirect air carrier approval procedures and ensure compliance with cargo security requirements. We recently completed a follow-up audit of FAA's Cargo Security Program. FAA has taken action to strengthen the program since September 11th by no longer allowing air carriers to accept cargo from unknown shippers and strengthening the requirements for becoming a known shipper. However, FAA has not taken actions to strengthen procedures for approving indirect air carriers to ship cargo on passenger aircraft, and weaknesses continue in this area.

This concludes my statement. I would be pleased to answer any questions.